13G36960-USA-AT

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月２３日

出願番号
Application Number: 特願２００３－１４６４９１

[ST. 10/C]: [ＪＰ２００３－１４６４９１]

出願人
Applicant(s): 株式会社東芝

２００４年　２月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１０４０７

【書類名】　特許願
【整理番号】　A000301122
【提出日】　平成15年 5月23日
【あて先】　特許庁長官　殿
【国際特許分類】　H01L 21/00
【発明の名称】　データ処理装置及び論理演算装置
【請求項の数】　16
【発明者】
　【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
　【氏名】　藤崎　浩一
【特許出願人】
　【識別番号】　000003078
　【氏名又は名称】　株式会社　東芝
【代理人】
　【識別番号】　100058479
　【弁理士】
　【氏名又は名称】　鈴江　武彦
　【電話番号】　03-3502-3181
【選任した代理人】
　【識別番号】　100091351
　【弁理士】
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【弁理士】
　【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100108855

【弁理士】

【氏名又は名称】　蔵田　昌俊

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ処理装置及び論理演算装置

【特許請求の範囲】

【請求項１】　入力側の複数本の信号線と、

出力側の複数本の信号線と、

前記入力側の複数本の信号線からデータを入力し、前記出力側の複数本の信号線へデータを出力する電子回路とを備え、

前記入力側の複数本の信号線から入力されるデータ及び前記出力側の複数本の信号線へ出力されるデータを、当該複数本の信号線のビット状態の組合せにより値が定まる１ビット・データとして扱うことを特徴とするデータ処理装置。

【請求項２】　前記１ビット・データの値として０を与える場合の前記複数本の信号線に係る第１のビット状態の組合せの持つハミング重みと、前記１ビット・データの値として１を与える場合の前記複数本の信号線に係る第２のビット状態の組合せの持つハミング重みとを均等又は概ね均等にすることを特徴とする請求項１に記載のデータ処理装置。

【請求項３】　前記複数本の信号線に係るビット状態の組み合わせとして、前記１ビット・データの値として０を与える第１のビット状態の組合せ又は０を与える第２のビット状態の組合せが入出力される稼働相と、無効なデータを表す前記第１又は第２のビット状態のいずれとも異なる第３のビット状態の組み合わせが入出力される休止相の区別を示す制御信号を入力する手段を更に備えたことを特徴とする請求項１に記載のデータ処理装置。

【請求項４】　予め定められた方法に従って前記稼働相の間に前記休止相が挿入されることを特徴とする請求項３に記載のデータ処理装置。

【請求項５】　各々の前記１ビット・データの入出力に係る前記稼働相の間にそれぞれ前記休止相が挿入されることを特徴とする請求項４に記載のデータ処理装置。

【請求項６】　前記第３のビット状態の組合せと前記第１のビット状態の組合せとの間のハミング距離と、前記第３のビット状態の組合せと前記第２のビット状態の組合せとの間のハミング距離とを均等又は概ね均等にすることを特徴と

する請求項３に記載のデータ処理装置。

【請求項７】　前記入力側及び出力側の信号線の本数をそれぞれ２本として、

前記第１のビット状態の組合せを、当該データに係る第１の信号線のビット状態が１であり且つ第２の信号線のビット状態が０である組合せ又は第１の信号線のビット状態が０であり且つ第２の信号線のビット状態が１である組合せのいずれかとし、

前記第２のビット状態の組合せを、前記第１のビット状態の組合せを反転させた組合せとし、

前記第３のビット状態の組合せを、前記第１の信号線のビット状態が０であり且つ第２の信号線のビット状態が０である第１の組合せ及び又は前記第１の信号線のビット状態が１であり且つ第２の信号線のビット状態が１である第２の組合せとすることを特徴とする請求項６に記載のデータ処理装置。

【請求項８】　前記データ処理装置は、同期信号を入力する手段を更に備え、

前記電子回路は、前記制御信号が前記稼動相を示す場合には、前記同期信号に従って、前記入力側の複数本の信号線から前記第１又は第２のビット状態の組み合わせに係る前記１ビット・データを入力し、前記出力側の複数本の信号線へ前記第１又は第２のビット状態の組み合わせに係る前記１ビット・データを出力することを特徴とする請求項３に記載のデータ処理装置。

【請求項９】　前記電子回路は、前記制御信号が前記休止相を示す場合には、前記入力側の複数本の信号線から前記無効なデータを入力することなしに、前記同期信号に従って、前記出力側の複数本の信号線から前記無効なデータを出力することを特徴とする請求項８に記載のデータ処理装置。

【請求項１０】　前記同期信号の立ち上がり又は立ち下がりの２回に１回の割合で、前記同期信号に同期した前記１ビット・データが入力されることを特徴とする請求項８に記載のデータ処理装置。

【請求項１１】　前記電子回路は、前記１ビット・データを保持する回路であることを特徴とする請求項１に記載のデータ処理装置。

【請求項１２】　第１及び第２の２本の信号線のビット状態の組合せにより値が定まる１ビット・データを入力し一旦保持した後に出力する第１のデータ保持回路と、

第１及び第２の２本の信号線のビット状態の組合せにより値が定まる１ビット・データを入力し一旦保持した後に出力する第２のデータ保持回路と、

前記第１のデータ処理装置の出力側の第１の信号線を第１の入力データとし、前記第２のデータ処理装置の出力側の第１の信号線を第２の入力データとし、該第１の入力データ及び該第２の入力データをもとにした第１の論理演算を行って、その結果を出力する第１の論理演算回路と、

前記第１のデータ処理装置の出力側の第２の信号線を第１の入力データとし、前記第２のデータ処理装置の出力側の第２の信号線を第２の入力データとし、該第１の入力データ及び該第２の入力データをもとにした第２の論理演算を行って、その結果を出力する第２の論理演算回路と、

前記第１の論理演算回路の出力側の信号線及び前記第２の論理演算回路の出力側の信号線の２本の信号線で与えられる第３のビット・データを入力し一旦保持した後に出力する第３のデータ保持回路とを備えたことを特徴とする論理演算装置。

【請求項１３】　前記第１の論理演算回路は、前記第１の入力データと前記第２の入力データとのＡＮＤ演算を行うものであり、

前記第２の論理演算回路は、前記第１の入力データと前記第２の入力データとのＯＲ演算を行うものであることを特徴とする請求項１２に記載の論理演算装置。

【請求項１４】　前記第１の論理演算回路は、前記第１の入力データと前記第２の入力データとのＯＲ演算を行うものであり、

前記第２の論理演算回路は、前記第１の入力データと前記第２の入力データとのＡＮＤ演算を行うものであることを特徴とする請求項１２に記載の論理演算装置。

【請求項１５】　前記第１の論理演算回路は、前記第１の入力データと前記第２の入力データとのＮＡＮＤ演算を行うものであり、

前記第２の論理演算回路は、前記第１の入力データと前記第２の入力データとのＮＯＲ演算を行うものであることを特徴とする請求項１２に記載の論理演算装置。

【請求項１６】　前記第１の論理演算回路は、前記第１の入力データと前記第２の入力データとのＮＯＲ演算を行うものであり、

前記第２の論理演算回路は、前記第１の入力データと前記第２の入力データとのＮＡＮＤ演算を行うものであることを特徴とする請求項１２に記載の論理演算装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データを処理するデータ処理装置及び論理演算を行う論理演算装置に関する。

【０００２】

【従来の技術】

マイクロコンピュータなどのように演算処理装置を備えたＬＳＩにおいて、暗号演算を行う際の演算処理中の消費電力を測定し、その消費電力からＬＳＩに納められている鍵情報を取り出すという電力差分攻撃(DPA:Differential Power Analysis)がある（例えば、非特許文献１参照）。

【０００３】

ＤＰＡによる攻撃では、最初に、複数のデータをＬＳＩに入力して、それぞれの消費電力を測定する。次に、暗号演算回路内にある鍵情報の推定を行う。この推定した鍵情報と消費電力との間に相関がある場合、その相関値を計算したとき、推定した値が正しいときに大きな相関値となり、推定が間違っているときに小さな相関値となる。ＤＰＡは、この原理を用いて、消費電力を測定することにより暗号演算回路内部の鍵情報を取り出すという攻撃方法である。

【０００４】

ＤＰＡによる攻撃は、破壊行為を伴わない攻撃であるため、外見を見ただけでは攻撃され鍵情報が取り出されたかどうか判断できず、不正利用による被害が拡

大するおそれがある。このため、暗号演算回路においてＤＰＡへの対策が必須となっている。

【０００５】

ところで、ＣＭＯＳ(Complemetary Metal-Oxide Semiconductor)デバイスを用いて製作された演算処理装置を備えたＬＳＩにおいては、同期信号を用い、１線で１ビットのデータを表している。このような回路構成のＬＳＩにおける消費電力は、ＣＭＯＳの特性により、処理しているデータ及びその前のデータに依存して変動する。

【０００６】

以下、ＣＭＯＳデバイスのＮＯＴ素子の動作と消費電力について説明する。

【０００７】

ＣＭＯＳによるＮＯＴ素子は、通常、供給電源線Ｖｃｃ、グランド線ＧＮＤ、ＶｃｃとＧＮＤとの間に直列に接続されたｎＭＯＳ及びｐＭＯＳ、両ＭＯＳのゲートに接続された入力信号線、ｎＭＯＳとＭＯＳとの接続線に接続された出力信号線、出力信号線とＧＮＤとの間に接続された容量Ｃを備えている。

【０００８】

このＮＯＴ素子の入力がｈｉｇｈ（もしくは、１）のとき、ｎＭＯＳが導通状態となるため、容量Ｃの正の電荷はｎＭＯＳを介してＧｎｄに流れるため、出力の電位はｌｏｗ（もしくは、０）になる。ここで、ｈｉｇｈとは、演算処理装置内で論理的に１と認識される電位であり、ｌｏｗとは０と認識される電位である。

【０００９】

逆に、入力がｌｏｗの場合、ｐＭＯＳが導通状態となる一方で、ｎＭＯＳは非通電状態となる。このｐＭＯＳが導通状態となることで、Ｖｃｃから正の電荷が容量Ｃに蓄積され、出力はｈｉｇｈとなる。

【００１０】

入力の遷移が起こらない場合、例えば入力がｈｉｇｈを維持する場合には、ｐＭＯＳが通電状態のままであり、出力はｌｏｗのままとなる。このとき、ｎＭＯＳは非導通状態であるためＧＮＤに電荷は流れず、電力は消費されない。他方、

入力がｌｏｗを維持する場合には、ｎＭＯＳが導通状態となり、出力はｈｉｇｈのままとなる。このとき、ｐＭＯＳは非導通状態であるので、電荷がＧＮＤに流れることはなく、電力は消費されない。

【００１１】

このように、ＣＭＯＳデバイスは、理想状態としては信号線の状態が変わらない場合には電力を消費しないため、ＣＭＯＳデバイスでＬＳＩを作ると低消費電力とすることができる。

【００１２】

さて、ＣＭＯＳデバイスは、状態が遷移するときに、Ｖｃｃから電荷が流れ、電力を消費する。このため、入力が遷移するＣＭＯＳデバイスと、入力が遷移しないＣＭＯＳデバイスとでは、消費する電力に差が生じる。このために、信号線の状態の遷移と鍵情報との間に関係がある場合、鍵情報の演算に関係して消費電力が変化する。この消費電力変動が外部から観測可能であり、このような場合、ＤＰＡにより鍵情報を特定されることになる。

【００１３】

理想的にはＣＭＯＳデバイスは信号の遷移以外に電力を消費しないが、実際には、信号の遷移による電力消費以外にも、洩れ電流という電流が流れることで、電力が消費される。この洩れ電流は、入力からｐＭＯＳ又はｎＭＯＳ１のゲートを通りドレインに流れたり、ＶｃｃからｐＭＯＳ及びｎＭＯＳ１を通ってＧＮＤ６に流れたりする電流である。この洩れ電流量は、ＣＭＯＳデバイスの入力信号線と出力信号線の状態に依存する。

【００１４】

以上説明したように、ＣＭＯＳデバイスを用いたマイクロコンピュータのデータ演算時の消費電力の変動は、信号線の状態遷移を伴わずに信号線の０，１の状態に応じて消費される電力と、遷移する信号線の数とに依存して決まる。

【００１５】

ＣＭＯＳデバイスを用いて、データを１ビットで表した回路構成の場合は、その前の状態により消費電力が変動することとなり、演算しているデータと消費電力との間に大きな相関を持つ。このため、鍵情報に関した演算を行っているとき

の消費電力の変動が、鍵情報と相関がある場合には、ＤＰＡによりマイクロコンピュータ内の鍵情報を推定されることとなる。

【００１６】

従来、ＤＰＡに対しては、演算中のデータをマスクして演算するという対策がある(例えば、特許文献１参照)。この対策は、鍵情報を用いた演算中の消費電力の変動が鍵情報と相関がなくなるように、鍵情報をマスクして演算を行うという方法である。このように鍵情報をマスクして演算することで、消費電力の変動と鍵情報との間の相関をなくすことでＤＰＡへの対策としている。このように、消費電力の変動と鍵情報との間の相関をなくすことが、ＤＰＡ対策として有効である。

【００１７】

しかし、この方法では、マスク演算のために余分なハードウェアあるいは計算時間が必要になる。

【００１８】

【特許文献１】

特開２０００－６６５８５

【００１９】

【非特許文献１】

Kocher, P, Jaffe, J, and Jun, B. Differential Power Analysis. In Advances in Cryptology of CRYPTO ´99 Springer- Verlag Lecture Notes in Computer Science 1666 p.388-398

【００２０】

【発明が解決しようとする課題】

ＤＰＡによる攻撃に対する対策としては、中間データを乱数でマスクするという手段を用いないで済ませるには、演算データによらず消費電力を同じにするという対策が考えられる。中間データの値によらず常に一定の消費電力を消費するような回路構成であるならば、消費電力の変動と鍵情報との間に相関はなくなるためにＤＰＡ対策となる。このような問題を解決するために、マイクロコンピュータ内において処理しているデータや、その前のデータに依存しない回路構成が

必要となる。しかしながら、そのための技術は未だ知られていない。

【００２１】

本発明は、上記事情を考慮してなされたもので、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができるデータ処理装置及び論理演算装置を提供することを目的とする。

【００２２】

【課題を解決するための手段】

本発明に係るデータ処理装置は、入力側の複数本の信号線と、出力側の複数本の信号線と、前記入力側の複数本の信号線からデータを入力し、前記出力側の複数本の信号線へデータを出力する電子回路とを備え、前記入力側の複数本の信号線から入力されるデータ及び前記出力側の複数本の信号線へ出力されるデータを、当該複数本の信号線のビット状態の組合せにより値が定まる１ビット・データとして扱うことを特徴とする。

【００２３】

好ましくは、前記１ビット・データの値として０を与える場合の前記複数本の信号線に係る第１のビット状態の組合せの持つハミング重みと、前記１ビット・データの値として１を与える場合の前記複数本の信号線に係る第２のビット状態の組合せの持つハミング重みとを均等又は概ね均等にするようにしてもよい。

【００２４】

これによって、静的消費電力をデータによらず一定又は概ね一定とすることができる。

【００２５】

また、好ましくは、前記複数本の信号線に係るビット状態の組み合わせとして、前記１ビット・データの値として０を与える第１のビット状態の組合せ又は０を与える第２のビット状態の組合せが入出力される稼働相と、無効なデータを表す前記第１又は第２のビット状態のいずれとも異なる第３のビット状態の組み合わせが入出力される休止相の区別を示す制御信号を入力する手段を更に備えるようにしてもよい。好ましくは、前記第３のビット状態の組合せと前記第１のビット状態の組合せとの間のハミング距離と、前記第３のビット状態の組合せと前記

第２のビット状態の組合せとの間のハミング距離とを均等又は概ね均等にするようにしてもよい。

【００２６】

これによって、静的消費電力及び動的消費電力をデータによらず一定又は概ね一定とすることができる。

【００２７】

また、本発明に係る論理演算回路は、第１及び第２の２本の信号線のビット状態の組合せにより値が定まる１ビット・データを入力し一旦保持した後に出力する第１のデータ保持回路と、第１及び第２の２本の信号線のビット状態の組合せにより値が定まる１ビット・データを入力し一旦保持した後に出力する第２のデータ保持回路と、前記第１のデータ処理装置の出力側の第１の信号線を第１の入力データとし、前記第２のデータ処理装置の出力側の第１の信号線を第２の入力データとし、該第１の入力データ及び該第２の入力データをもとにした第１の論理演算を行って、その結果を出力する第１の論理演算回路と、前記第１のデータ処理装置の出力側の第２の信号線を第１の入力データとし、前記第２のデータ処理装置の出力側の第２の信号線を第２の入力データとし、該第１の入力データ及び該第２の入力データをもとにした第２の論理演算を行って、その結果を出力する第２の論理演算回路と、前記第１の論理演算回路の出力側の信号線及び前記第２の論理演算回路の出力側の信号線の２本の信号線で与えられる第３のビット・データを入力し一旦保持した後に出力する第３のデータ保持回路とを備えたことを特徴とする。

【００２８】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００２９】

本発明によれば、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができる。

【００３０】

従って、本発明に係る装置を暗号演算回路に適用すれば、電力差分攻撃へ対策

することができる。

【００３１】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００３２】

最初に、本実施形態の基本的な構成について説明する。

【００３３】

本実施形態では、データパス部のハミング重みを一定（または、ほぼ一定）にするために、従来は１本の信号線で１ビットを表現していたものを、１ビットのデータを表すのに信号線を２本以上用いる。

【００３４】

すなわち、ｎ（ｎは２以上）本の信号線で与えられるデータを、ｎビットのデータとして扱うのではなく、当該ｎ本の信号線のビット状態の組合せにより値が定まる１ビット・データとして扱う。

【００３５】

なお、以下では、１ビットのデータを表すのに信号線を２本用いる構成を中心に説明する。

【００３６】

従来のように１本の信号線で１ビットのデータを表す場合、信号線の１または０の状態がそのまま１ビットのデータの値に対応するが、１ビットのデータを表すのに２本の信号線を用いて表現する場合のデータの表現方法としては、２本の信号線を組み合わせて、１線式において“ｈｉｇｈ（もしくは、１）”と表した状態（当該ビットの値＝１に対応する状態）を２線式では（１，０）と符号化して表し（すなわち、第１の信号線が状態１をとり、第２の信号線が状態０をとる）、１線式において“ｌｏｗ（もしくは、０）”と表した状態（当該ビットの値＝０に対応する状態）を（０，１）と符号化して表す（すなわち、第１の信号線が状態０をとり、第２の信号線が状態１をとる）、といった表現方法を導入する。もちろん、１線式において“１”と表した状態を２線式では（０，１）で、“０”と表した状態を（１，０）で表す表現方法も可能である。これらの場合、デ

ータパス部のハミング重みは１で一定となる。

【００３７】

このようにデータパス部のデータを符号化し、１ビットを２本の信号線で表すという２線化を行うことで、ＣＭＯＳデバイスを用いて製作された演算処理装置内において、データの内容にかかわらずに、鍵情報を演算するデータパス部における状態１を持つ信号線の数と、状態０を持つ信号線の数とを等しくすることができる。

【００３８】

データパス部におけるハミング重み（状態１を持つ信号線の数）を一定にすることができる理由を説明する。従来のように１線で１ビットを表す１線式では、ビット値＝０を表すときのハミング重みは０となり、ビット値＝１を表すときのハミング重みは１となる。他方、本実施形態のように例えば２本の信号線で１ビットを表現する２線式では、ビット値＝０を表すときのハミング重みとビット値＝１を表すときのハミング重みはいずれも１となる。このように、２線式では、データの内容にかかわらずにハミング重みは同じ値になるため、データパス部のハミング重みは演算中に一定となるのである。

【００３９】

信号線の遷移に伴わずに消費される電力（スタティック消費電力）は、データパス部のハミング重みに依存することから、２線式にすることでデータによらずスタティック消費電力を一定とすることが可能となる。これによって、スタティック消費電力と鍵情報との間の相関をなくすことができる。

【００４０】

従って、このような構成を暗号演算回路に適用すれば、電力差分攻撃へ対策することができる。

【００４１】

また、本実施形態では、次のようにデータが有効であるフェイズ（稼働相）とデータが無効であるフェイズ（休止相）とを設ける２相方式を採用すると好ましい。

【００４２】

まず、上記のように符号化された有効なデータがデータパス部を流れるときを稼働相とする。また、状態遷移する信号線の数を一定（または、ほぼ一定）にするため無効なデータ（非データ）がデータパス部を流れるときを休止相とする。

【００４３】

例えば、２線式において、１ビットのデータが上記のように（１，０）または（０，１）で表されるのに対して、それらのいずれとの間の遷移についてもハミング距離を同じくする（０，０）または（１，１）を非データとする。（０，０）は第１及び第２の信号線がいずれも状態０をとり、（１，１）は第１及び第２の信号線がいずれも状態１をとるものである。

【００４４】

このように、稼働相のときにデータを流し、休止相のときに非データを流すようにすることで、休止相を挟んで隣接するデータ間の依存関係をなくすることができる。これは、休止相により１ビットを表す２本の信号線が（０，０）または（１，１）という非データを表す状態に遷移するため、後続するデータは、直前のデータ（休止相を挟んで隣接するデータ）とは無関係となり、休止相にある非データとの間の相違だけで関係するからである。

【００４５】

また、２線化された信号線を（１，０）または（０，１）という本来のデータの状態から一旦（０，０）または（１，１）という本来のデータではない非データの状態に遷移させることで、データの内容によらずに１から０または０から１へ状態遷移する信号線の数を一定にし、これによって、データの内容によらず信号線の遷移による消費電力（ダイナミック消費電力）を一定とすることができる。この結果、ダイナミック消費電力と鍵情報との間の相関をなくすことができる。

【００４６】

従って、このような構成を暗号演算回路に適用すれば、電力差分攻撃へ対策することができる。

【００４７】

ここで、稼働相と休止相とを例えば交互に設けた場合を考える。例えば、図２

にあるように、同期信号ＣＬＫの立ち上がりのタイミングに合わせて、制御信号線をｈｉｇｈ，ｌｏｗと交互に繰り返すようにし、この制御信号に従ってデータパス部を稼働相と休止相が交互に繰り返すようにする（なお、図２では稼働相と休止相とを同期信号ＣＬＫの立ち下がりのタイミングで切り替えたが、同期信号ＣＬＫの立ち下がりのタイミングで切り替えるようにしてもよい）。

【００４８】

この場合、稼働相における信号線の状態は（１，０）または（０，１）であり、休止相における信号線の状態は（０，０）または（１，１）であるので、遷移状態としては、稼働相から休止相への遷移では、（１，０）→（０，０）、（１，０）→（１，１）、（０，１）→（０，０）、または（０，１）→（１，１）、休止相から稼働相への遷移では、（０，０）→（１，０）、（０，０）→（０，１）、（１，１）→（１，０）、（１，１）→（０，１）となり、いずれも、状態遷移する信号線の数は１つで一定となる。

【００４９】

なお、上記した２線式２相方式の回路構成において、同期信号の立ち上がり（または、立ち下がり）において休止相とするために、データを保持するレジスタは、休止相のデータを内部で保持しないように、入力信号を監視し、休止相であり非データを検出した場合には、レジスタの入力を内部に取り込まないようにし、他方、稼働相のデータを検出した場合には、同期信号の立ち上がり（または、立ち下がり）において入力を内部に取り込むようにするという回路構成にするのが望ましい。

【００５０】

また、休止相または稼働相を示す制御信号線を用意し、休止相の場合にはデータパス部に非データが流れるようにレジスタの出力部にＡＮＤ素子またはＯＲ素子を入れ、制御信号線に応じて、非データがレジスタの先にある組合せ回路へ入力されるようにしてもよい。

【００５１】

以下では、２線式２相方式の回路の具体例をいくつか示す。

【００５２】

最初に、稼働相において入力データを内部に保持し、休止相においては入力データを取り込まない２線式２相方式のデータ保持回路（レジスタ）の構成例について説明する。

【００５３】

図１に、２線化されたデータを保持するデータ保持回路の構成例を示す。本データ保持回路は、第１のレジスタ１と、第２のレジスタ２と、監視回路３と、第１のＡＮＤ回路６と、第２のＡＮＤ回路７とを含む。監視回路３は、ＯＲ回路４とＡＮＤ回路５とを含む。なお、図３に、第１及び第２のレジスタ１，２として使用可能な、１つのＡＮＤ回路１１と６つのＮＡＮＤ回路１２～１７からなるエッジトリガ型Ｄフリップフロップの例を示す。また、レジスタ１，２には、マスタースレーブ型Ｄフリップフロップを用いることも可能である。

【００５４】

なお、本データ保持回路は、非データ（０，０）を休止相とする場合の例である。もちろん、図１を修正すれば非データ（１，１）を休止相とする場合も実現可能である。

【００５５】

図１において、制御信号ＣＴＲＬと同期信号ＣＬＫには、例えば図２の信号がそれぞれ供給される（本例の場合、ＣＴＲＬがｈｉｇｈのとき稼動相となり、ｌｏｗのとき休止相となる）。

【００５６】

図１に示されるように、２線に符号化されたデータを保持するために、従来の１線式で使われるＤフリップフロップを用いて実現することができる。このように２つのＤフリップフロップ１，２を並べることで、２線に符号化されたデータを保持することができる。

【００５７】

監視回路９は、休止相であることを監視するための回路である。すなわち、例えばデータパス部の信号線が（０，０）になる場合が休止相とした場合、監視回路９は図１のようにＯＲ回路４とＡＮＤ回路５で実現することができる。なお、（１，１）を休止相とした場合には、ＮＡＮＤ素子とＡＮＤ素子で実現すること

ができる。

【００５８】

第１のＡＮＤ回路６及び第２のＡＮＤ回路７の出力が、当該２線式の出力となる。図１の例では、稼動相において、（１，０）または（０，１）が出力され、休止相において（０，０）が出力される。

【００５９】

図４に、本データ保持回路の動作を表すタイミングチャート例を示す。なお、図４において、（Ｉ１，Ｉ２）は図１の入力Ｉ１，Ｉ２の各状態を示し、（Ｒ１，Ｒ２）は図１の各レジスタ１，２の保持状態を示し、（Ｏ１，Ｏ２）は図１の出力Ｏ１，Ｏ２の各状態を示す。稼動相で入力された入力データは、次の休止相の間も保持され（すなわち、休止相の非データは取り込まれない）、次の稼動相で出力されることがわかる。

【００６０】

以上のように本構成例によれば、休止相において非データを取り込まず、稼働相においてデータを保持し、稼動相においてデータを出力し、休止相において非データを出力するようなデータ保持回路を実現することができる。

【００６１】

ところで、データ保持回路の実現方法としては、図１の構成例のように既存の１線式で用いられているＤフリップフロップを用いて実現する方法もあるが、これよりも少ない論理素子で実現することも可能である。

【００６２】

図５に、この場合のデータ保持回路の構成例を示す。図５に示されるように、本データ保持回路は、ＯＲ回路ｏｒ１、ＡＮＤ回路ａ１～ａ４、ＮＡＮＤ回路ｎａ１～ｎａ６を含む（なお、ＯＲ回路ｏｒ１とＡＮＤ回路ａ１で監視回路３を形成している）。

【００６３】

なお、図５は、休止相が（０，０）である場合の構成例を示しているが、もちろん、図５を修正すれば休止相が（１，１）である場合も実現可能である。

【００６４】

ここで、図６及び図７を用いて、図５に例示した２線式２相方式のデータ保持回路の動作について詳しく説明する。なお、図６及び図７では、図５のＡＮＤ回路ａ３，ａ４は省略している。

【００６５】

最初に図５の回路が休止相の状態にあるとし、入力Ｉ１，Ｉ２ともに０であったとする。

【００６６】

次いで稼働相に遷移し、図６のように入力Ｉ２が“１”に遷移したとすると、ｏｒ１の出力は“０”から“１”に遷移する。そして図６のように同期信号ＣＬＫが“０”から“１”に立ち上がることで、ＡＮＤ素子ａ１の出力が“０”から“１”に遷移する。これにより、ＮＡＮＤ素子ｎａ２の出力が“１”から“０”に遷移する。ＡＮＤ素子ａ２の出力は、“０”となりＮＡＮＤ素子ｎａ３の出力は“１”に遷移する。以上の動作で、ＮＡＮＤ素子ｎａ５の出力は“１”となり、ＮＡＮＤ素子ｎａ６の出力は“０”となる。ＮＡＮＤ素子ｎａ５，ｎ６の出力をＡＮＤ素子ａ４，ａ３の入力に入れ、制御信号ＣＴＲＬとのＡＮＤ演算を行うことで、稼動相におけるデータ（０，１）が出力される。

【００６７】

さらに稼働相から休止相へ遷移し、図７のように入力Ｉ２が“１”から“０”に遷移する。この結果、ＯＲ素子ｏｒ１の出力は“０”になり、ＡＮＤ素子ａ１，ａ２の出力も“０”となる。ＡＮＤ素子ａ１の出力が“０”になることで、ＮＡＮＤ素子ｎａ２の出力は“１”となり、ＮＡＮＤ素子ｎａ３の出力も“１”となる。このとき、ＮＡＮＤ素子ｎａ５，ＮＡＮＤ素子ｎａ６の出力は変わらない。ＮＡＮＤ素子ｎａ５，ｎ６の出力はＡＮＤ素子ａ４，ａ３の入力に入れられるが、制御信号ＣＴＲＬとのＡＮＤ演算が行われるので、稼動相におけるデータ（０，０）が出力される。

【００６８】

以上に示したように、図５のような回路構成とすることで、休止相において入力を取り込まず以前の稼働相のデータを保持し続け、稼働相において入力データを内部に取り込むような２線式用の１ビットのデータ保持回路を構成することが

できる。

【００６９】

このようなレジスタを用い、稼働相と休止相を交互に流すことで、データパス部のハミング重みが一定となるとともに、信号線の遷移数が一定になることについて説明する。

【００７０】

スタティック消費電力においては、データのハミング重みが問題となる。２線式のデータパス部において、１ビットのデータは（１，０）または（０，１）と表現される。例えば、１線式において、８ビットのデータ０ｘ１８（０００１１０００）についてはハミング重みは“２”、０ｘｆｆ（１１１１１１１１）についてはハミング重みは“８”となる。一方、２線式においては、８ビットのデータ０ｘ１８は（０，１）（０，１）（０，１）（１，０）（１，０）（０，１）（０，１）（０，１）と表されるために、そのハミング重みは“８”であり、０ｘｆｆは（１，０）（１，０）（１，０）（１，０）（１，０）（１，０）（１，０）（１，０）と表されるために、そのハミング重みは同じく“８”となる。

【００７１】

このように、１線式ではデータの内容によってハミング重みが異なるが、２線式では１ビットのデータを２線で（１，０）または（０，１）で表すために、データの内容にかかわらずにハミング重みは一定となる。

【００７２】

次に、図８に、１ビットの論理ＡＮＤ演算を行う２線式データパス部の構成例を示す。

【００７３】

図８に示されるように、本演算回路は、本実施形態のデータ保持回路ｒ１～ｒ３と、ＡＮＤ回路ａ１と、ＯＲ回路ｏｒ１とを含む。

【００７４】

以下、図８に例示した１ビットの論理ＡＮＤ演算を行う２線式データパス部を用いて、ダイナミック消費電力について説明する。

【００７５】

ここでは、１ビットのデータの値＝１を（１，０）で表し、１ビットのデータの値＝０を（０，１）で表すものとする。また、休止相を（０，０）とする。また、制御信号ＣＴＲＬと同期信号ＣＬＫには図２の信号がそれぞれ供給されるものとする（ＣＴＲＬがｈｉｇｈのとき稼動相となり、ｌｏｗのとき休止相となるものとする）。

【００７６】

まず、図９の状態において、レジスタｒ１に（０，１）、レジスタｒ２に（１，０）、レジスタｒ３に（１，０）がそれぞれ保持されており、休止相（制御信号は“０”）であったとする。この状態では、全ての信号線の状態が“０”になっている。

【００７７】

次に、休止相から稼働相へ遷移し（制御信号は“０”から“１”に遷移し）、図１０の状態になったものとする。この状態では、レジスタｒ１へ（１，０）、レジスタｒ２へ（１，０）がそれぞれ入力されたものとする。また、レジスタｒ１から（０，１）、レジスタｒ２から（１，０）がそれぞれ出力され、それらが２線式のデータに対する論理ＡＮＤ演算を行う組合せ回路ａ１，ｏｒ１に入力され、その演算結果（０，１）が出力され、これがレジスタｒ３に届き、保持される。また、レジスタｒ３からは、（１，０）が出力される。

【００７８】

ここで、図９の状態から図１０の状態への遷移をみると、組合せ回路の６つ信号線のうちの３つの信号線において状態が“０”から“１”に遷移していることがわかる。

【００７９】

次に、稼働相から休止相へ遷移し（制御信号は“１”から“０”に遷移し）、図９の状態に戻ったものとする。この状態では、全ての信号線の状態が“０”になっている。

【００８０】

ここで、図１０の状態から図９の状態への遷移をみると、やはり３つの信号線において状態が遷移していることがわかる。

【００８１】

次に、休止相から稼働相へ遷移し（制御信号は“０”から“１”に遷移し）、図１１の状態になったものとする。この状態では、レジスタｒ１へ（０，１）、レジスタｒ２へ（０，１）がそれぞれ入力されたものとする。また、レジスタｒ１から（１，０）、レジスタｒ２から（１，０）がそれぞれ出力され、それらが２線式のデータに対する論理ＡＮＤ演算を行う組合せ回路ａ１，ｏｒ１に入力され、その演算結果（１，０）が出力され、これがレジスタｒ３に届き、保持される。また、レジスタｒ３からは、（０，１）が出力される。

【００８２】

ここで、図９の状態から図１１の状態への遷移をみると、やはり３つの信号線において状態が遷移していることがわかる。

【００８３】

このように、データの内容にかかわらずに、遷移する信号線の数は一定になる。

【００８４】

このように、稼働相と休止相によりデータと非データを交互にデータパスに流すことで、データパス部における組合せ回路の信号線のうち状態遷移するものの個数は一定となり、ダイナミック消費電力は一定となる。

【００８５】

ところで、図８では１ビットの論理ＡＮＤ演算を行う２線式データパス部の構成例を示したが、もちろん、この構成例を適宜修正することによって、他の論理演算を行う２線式データパス部も実現可能である。

【００８６】

図１２に、１ビットの論理ＯＲ演算を行う２線式データパス部の構成例を示す。図１２に示されるように、本演算回路は、本実施形態のデータ保持回路ｒ１～ｒ３と、ＯＲ回路ｏｒ２とＡＮＤ回路ａ２とを含む。

【００８７】

また、図１３に、１ビットの論理ＮＡＮＤ演算を行う２線式データパス部の構成例を示す。図１３に示されるように、本演算回路は、本実施形態のデータ保持

回路ｒ１～ｒ３と、ＮＡＮＤ回路ｎａ１と、ＮＯＲ回路ｎｏｒ１とを含む。

【００８８】

また、図１４に、１ビットの論理ＮＯＲ演算を行う２線式データパス部の構成例を示す。図１４に示されるように、本演算回路は、本実施形態のデータ保持回路ｒ１～ｒ３と、ＮＯＲ回路ｎｏｒ２とＮＡＮＤ回路ｎａ２とを含む。

【００８９】

また、図１５に、１ビットの論理ＮＯＴ演算を行う２線式データパス部の構成例を示す。図１５に示されるように、本演算回路は、本実施形態のデータ保持回路ｒ１，ｒ２とを含み、データ保持回路ｒ１の第１の出力Ｏ１をデータ保持回路ｒ２の第２の入力Ｉ１へ結合し、データ保持回路ｒ１の第２の出力Ｏ２をデータ保持回路ｒ２の第１の入力Ｉ２へ結合するものである（図中、ｈ１の配線部分参照）。なお、この場合、１ビットの論理ＮＯＴ演算を行う２線式データパス部は、図１６に示すように、２つのＮＯＴ回路ｎｏｔ１，ｎｏｔ２を用いても実現可能である。

【００９０】

なお、これまでの説明では、非データ（０，０）を休止相とする場合を中心に説明したが、非データ（１，１）を休止相とする場合も実現可能であり、また、休止相に非データ（０，０）と（１，１）を併用する（例えば、交互あるいはランダムに使用する）構成も可能である。

【００９１】

また、これまでの説明では、稼動相と休止相とを交互に設ける場合を中心に説明したが、所定回数の稼動相が続いた後に休止相を設ける、休止相をランダムに設けるなど、それ以外の構成も可能である。

【００９２】

また、これまでの説明では、１ビットのデータを表すのに信号線を２本用いる構成を中心に説明したが、１ビットのデータを表すのに信号線を３本以上用いる構成も可能である。

【００９３】

１ビットのデータを表すのに４本の信号線を用いる場合には、例えば、状態１

を（１，１，０，０）、状態０を（０，０，１，１）で表し、５本の信号線を用いる場合には、例えば、状態１を（１，０，１，０，１）、状態０を（０，１，０，１，０）で表すなどすればよい。

【００９４】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

【００９５】

【発明の効果】

本発明によれば、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係るデータ保持回路の構成例を示す図

【図２】　同実施形態における同期信号と制御信号のタイミングの一例を示す図

【図３】　同期信号を用いた１線式の１ビットのＤフリップフロップの構成例を示す図

【図４】　同実施形態に係るデータ保持回路の動作例を示す図

【図５】　本発明の一実施形態に係るデータ保持回路の他の構成例を示す図

【図６】　図５のデータ保持回路の動作について説明するための図

【図７】　図５のデータ保持回路の動作について説明するための図

【図８】　同実施形態に係る論理ＡＮＤ演算を行うデータパス部の構成例を示す図

【図９】　図８のデータパス部の動作について説明するための図

【図１０】　図８のデータパス部の動作について説明するための図

【図１１】　図８のデータパス部の動作について説明するための図

【図１２】　同実施形態に係る論理ＯＲ演算を行うデータパス部の構成例を示す図

【図１３】　同実施形態に係る論理ＮＡＮＤ演算を行うデータパス部の構成例を示す図

【図１４】　同実施形態に係る論理ＮＯＲ演算を行うデータパス部の構成例を示す図

【図１５】　同実施形態に係る論理ＮＯＴ演算を行うデータパス部の構成例を示す図

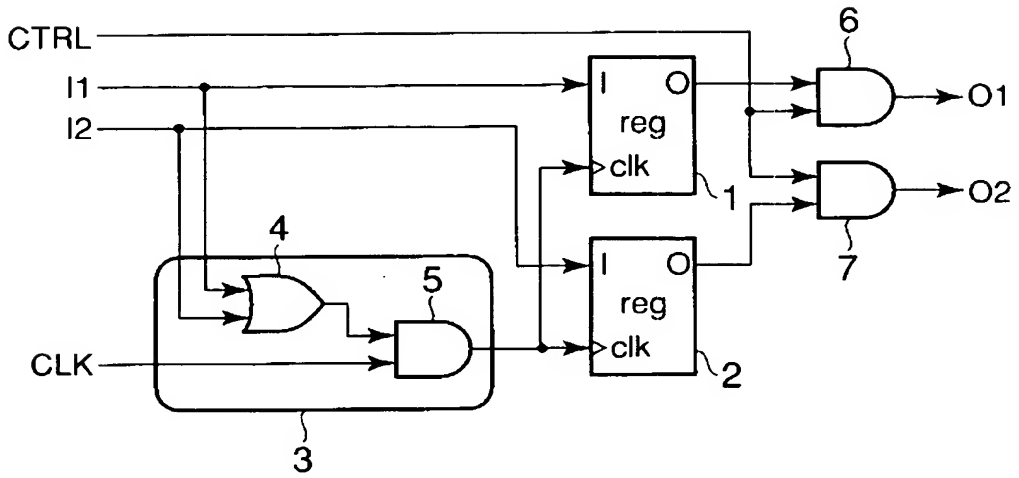
【図１６】　同実施形態に係る論理ＮＯＴ演算を行うデータパス部の他の構成例を示す図

【符号の説明】

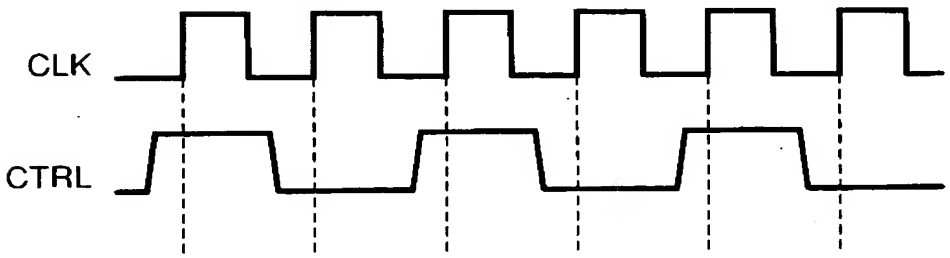
１，２…レジスタ、３…監視回路、５，６，７，１１，ａ１～ａ４…ＡＮＤ回路、４，ｏｒ１，ｏｒ２…ＯＲ回路、１２～１７，ｎａ１～ｎａ６…ＮＡＮＤ回路、ｎｏｒ１，ｎｏｒ２…ＮＯＲ回路、ｎｏｔ１，ｎｏｔ２…ＮＯＴ回路、ｒ１～ｒ３…データ保持回路

【書類名】　図面

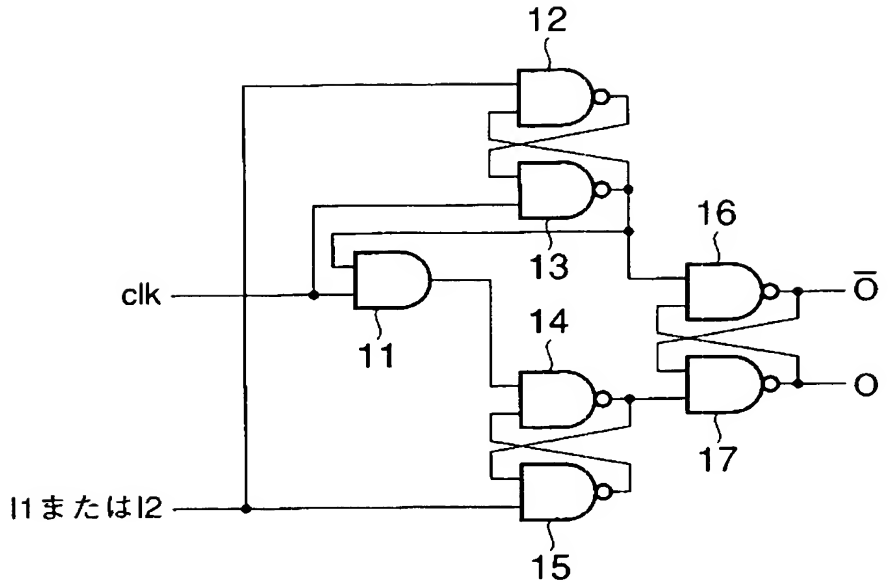
【図１】



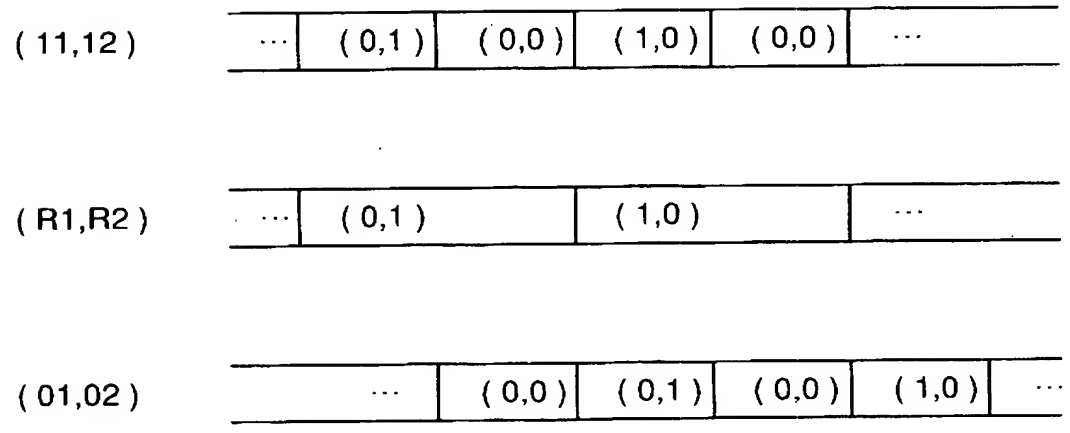
【図２】



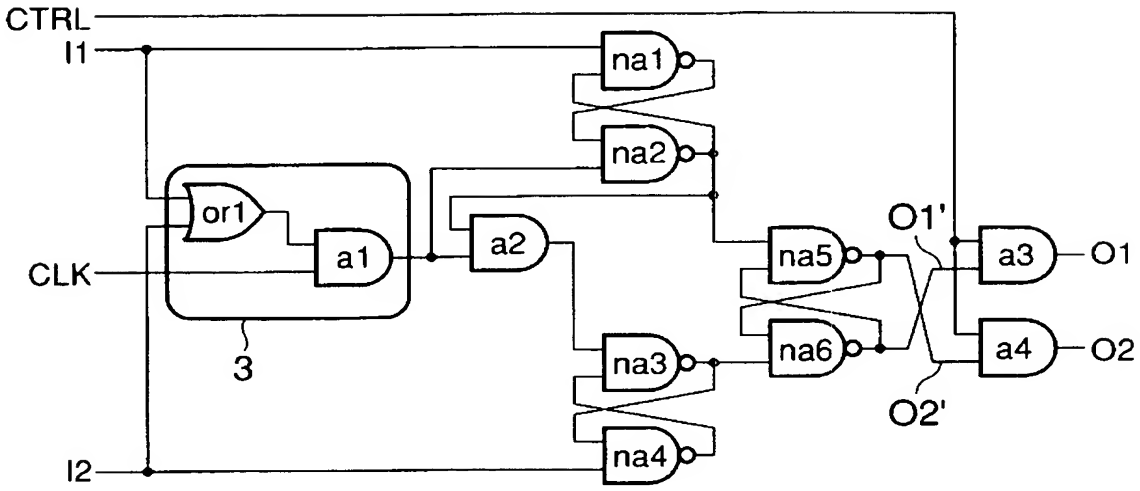
【図３】


12
16
13
clk
11
14
O
17
I1またはI2
15

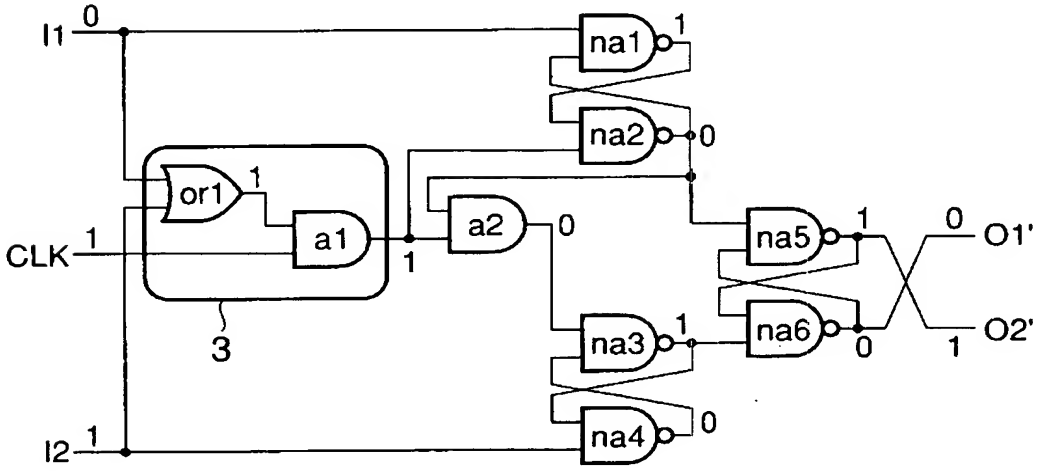
【図４】


(11,12)
…
(0,1)
(0,0)
(1,0)
(0,0)
…
(R1,R2)
…
(0,1)
(1,0)
…
(01,02)
…
(0,0)
(0,1)
(0,0)
(1,0)
…

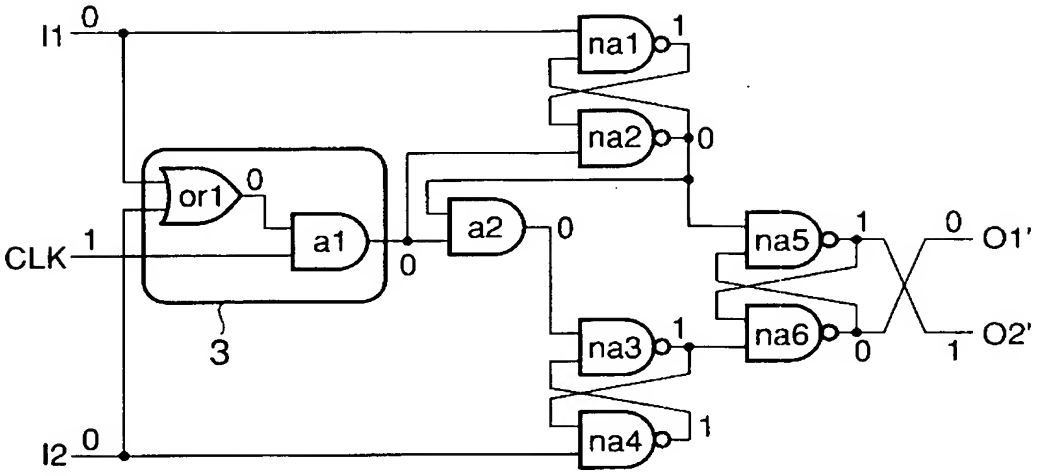
【図５】


CTRL
I1
CLK
I2
or1
a1
3
a2
na1
na2
na3
na4
na5
na6
O1'
O2'
a3
a4
O1
O2

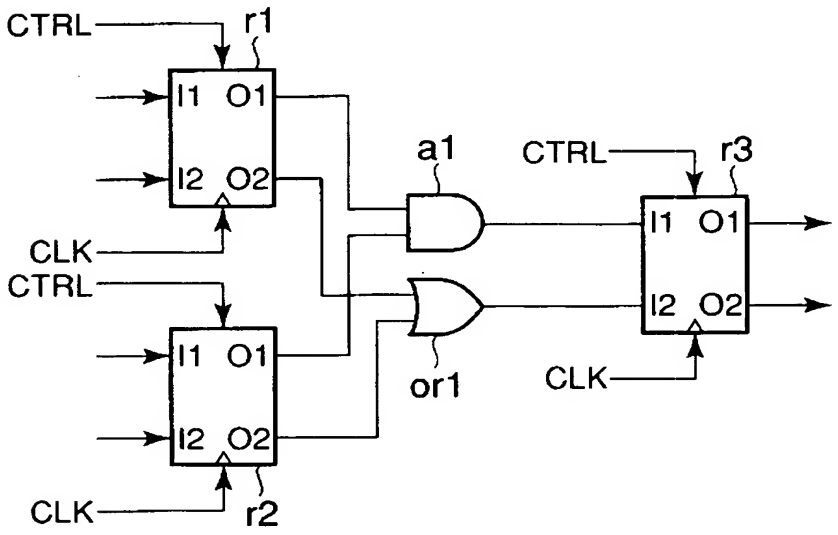
【図６】


I1
0
CLK
1
I2
1
or1
1
a1
3
a2
1
0
na1
1
na2
0
na3
1
na4
0
na5
1
na6
0
0
1
O1'
O2'

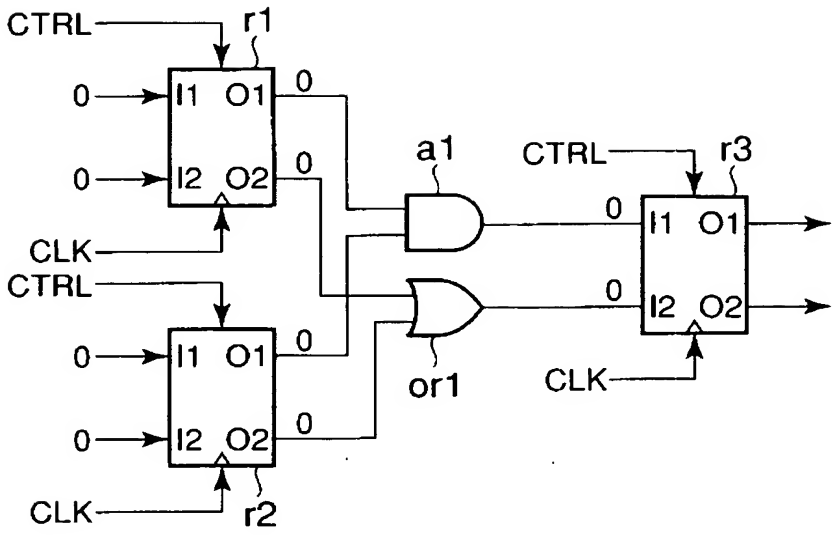
【図７】


I1
0
CLK
1
I2
0
or1
0
a1
a2
0
0
3
na1
1
na2
0
na3
1
na4
1
na5
1
na6
0
0
1
0
O1'
O2'

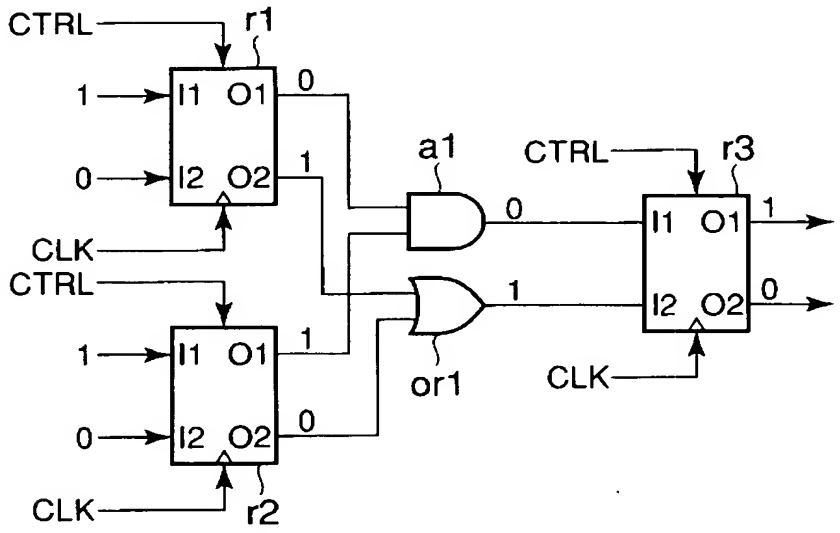
【図８】


CTRL
r1
I1 O1
I2 O2
CLK
CTRL
I1 O1
I2 O2
CLK
r2
a1
or1
CTRL
r3
I1 O1
I2 O2
CLK

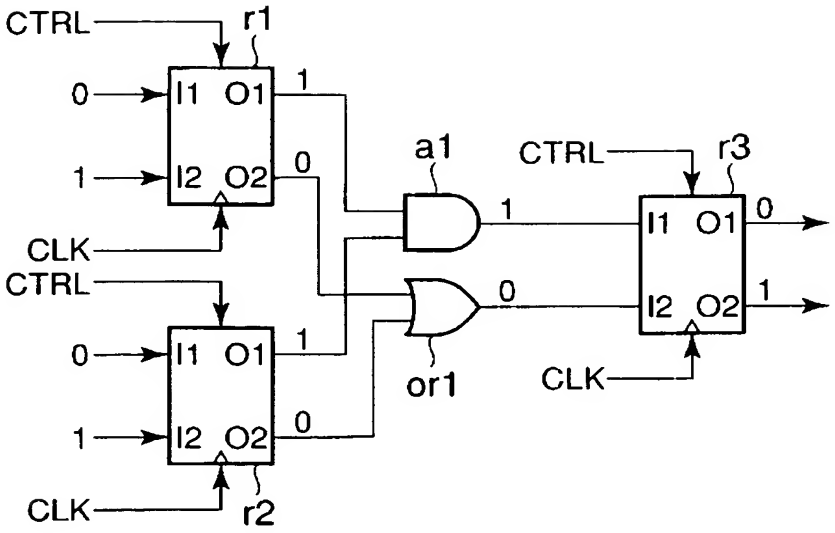
【図９】


CTRL
r1
I1 O1
I2 O2
0
0
0
0
CLK
CTRL
0
0
0
0
CLK
r2
a1
or1
CTRL
r3
0
0
I1 O1
I2 O2
CLK

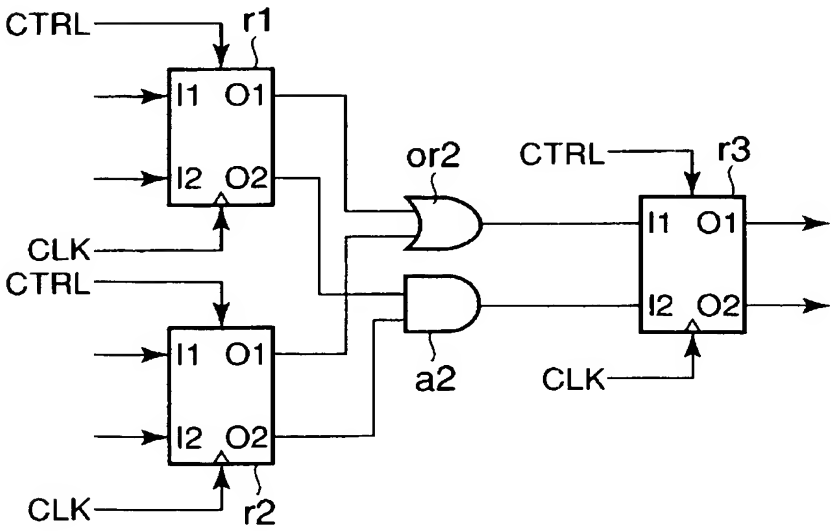
【図１０】


CTRL
r1
1
0
I1 O1
I2 O2
0
1
CLK
CTRL
1
0
1
0
CLK
r2
a1
or1
CTRL
r3
0
1
I1 O1
I2 O2
1
0
CLK

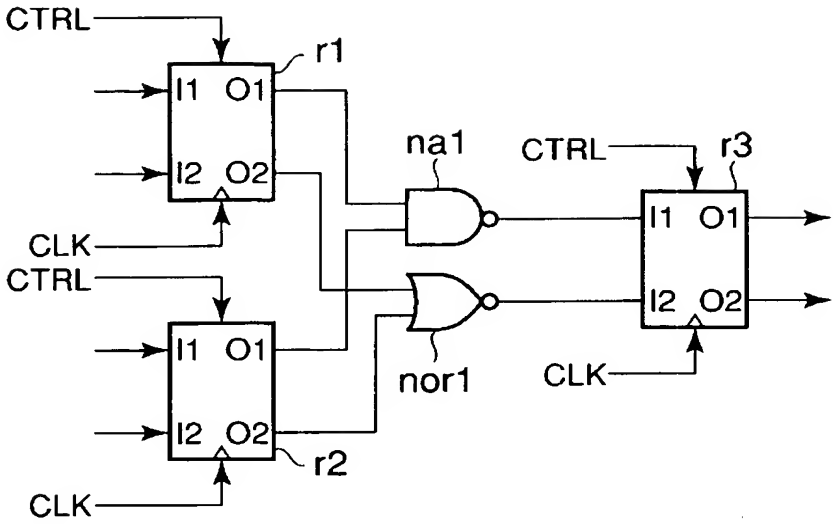
【図１１】


CTRL
r1
0
1
I1 O1
I2 O2
1
0
CLK
CTRL
0
1
I1 O1
I2 O2
1
0
CLK
r2
a1
or1
CTRL
r3
1
0
I1 O1
I2 O2
0
1
CLK

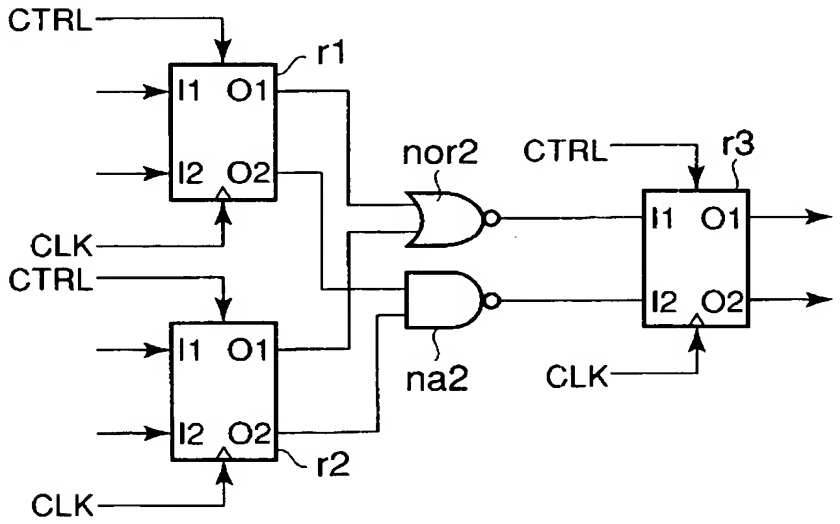
【図１２】


CTRL
r1
I1 O1
I2 O2
CLK
CTRL
I1 O1
I2 O2
CLK
r2
or2
a2
CTRL
r3
I1 O1
I2 O2
CLK

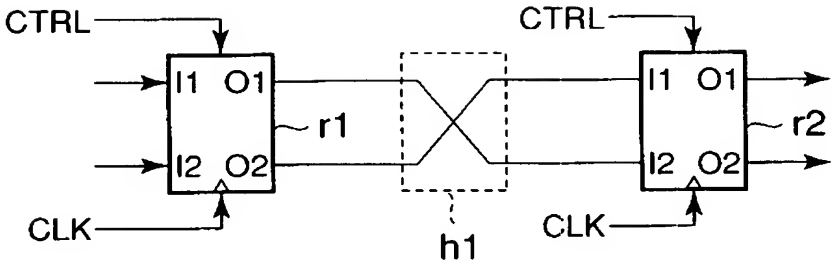
【図１３】


CTRL
r1
I1 O1
I2 O2
CLK
CTRL
I1 O1
I2 O2
r2
CLK
na1
nor1
CTRL
r3
I1 O1
I2 O2
CLK

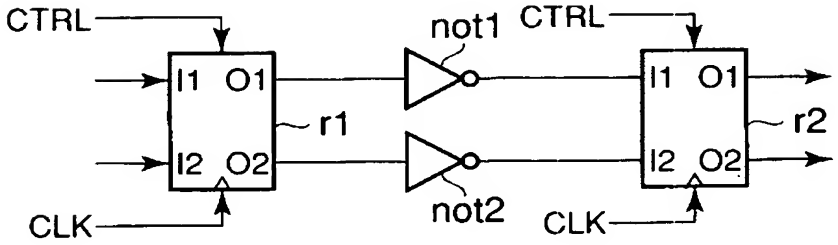
【図１４】


CTRL
r1
I1 O1
I2 O2
CLK
CTRL
I1 O1
I2 O2
r2
CLK
nor2
na2
CTRL
r3
I1 O1
I2 O2
CLK

【図１５】


CTRL
I1 O1
I2 O2
r1
CLK
h1
CTRL
I1 O1
I2 O2
r2
CLK

【図１６】


CTRL
I1 O1
I2 O2
r1
CLK
not1
not2
CTRL
I1 O1
I2 O2
r2
CLK

【書類名】　　要約書

【要約】

【課題】　演算対象となるデータの内容によらずに消費電力を一定とすることができるデータ処理装置を提供すること。

【解決手段】　入力側の２本の信号線Ｉ１，Ｉ２あるいは出力側の２本の信号線Ｏ１，Ｏ２の状態が（１，０）である場合を値１を持つ１ビット・データとし、（０，１）である場合を値０を持つ１ビット・データとし、レジスタ１，２は、ＣＴＬＲ信号がｈｉｇｈの状態で、（１，０）又は（０，１）で表される１ビット・データをＣＬＫ信号に従って入力し一旦保持するとともに、保持していた（１，０）又は（０，１）で表される１ビット・データを出力する。他方、ＣＴＬＲ信号がｌｏｗの状態では、（０，０）で表される無効なデータが与えられるが、レジスタ１，２は、該無効なデータは取り込まない。また、このとき、ＡＮＤ回路６，７により、無効なデータ（０，０）が出力される。

【選択図】　　図１

特願２００３－１４６４９１

出　願　人　履　歴　情　報

識別番号　［０００００３０７８］

１．変更年月日　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝